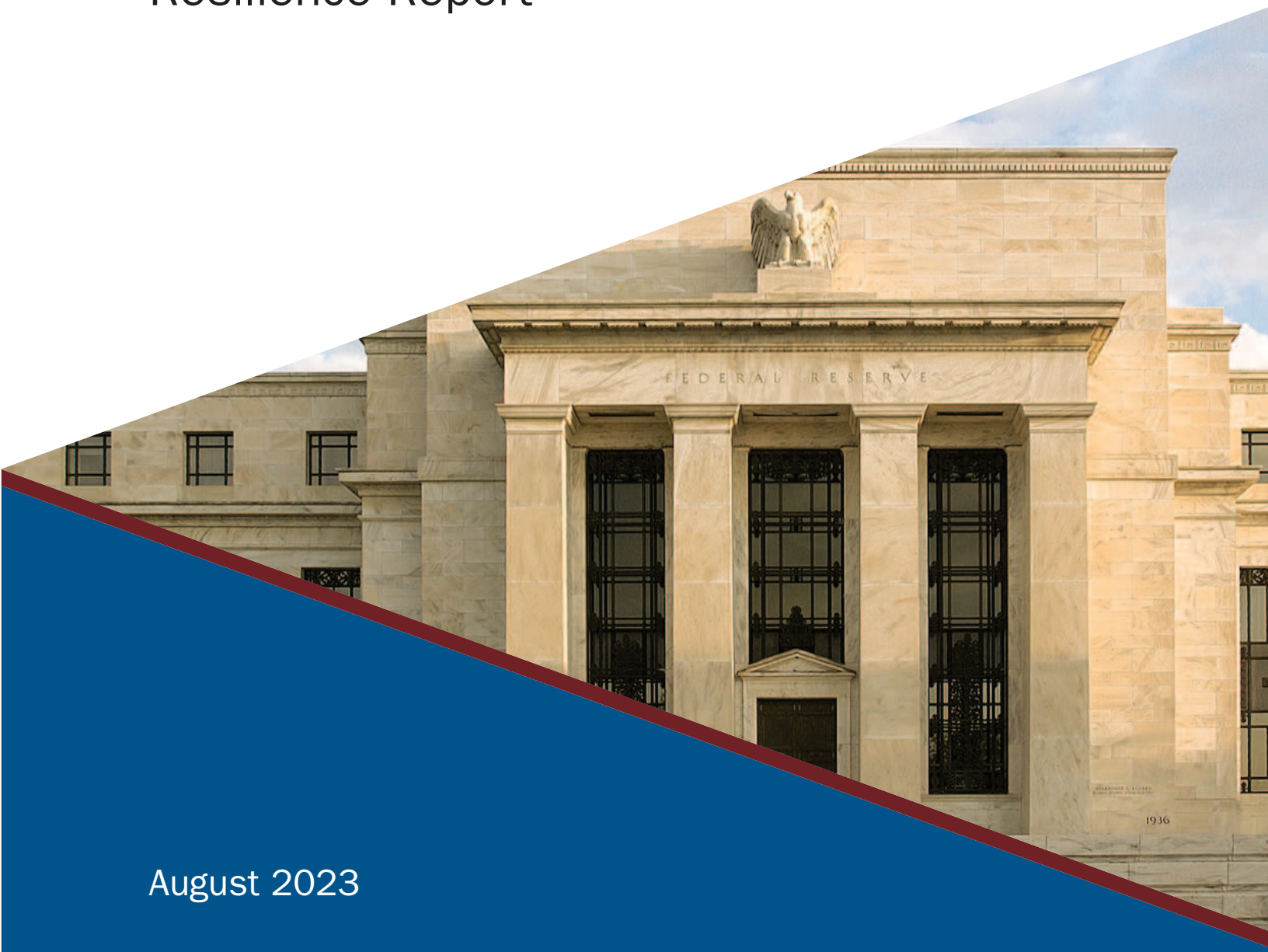
REPORT TO CONGRESS

Cybersecurity and Financial System Resilience Report



August 2023

BOARD OF GOVERNORS OF THE FEDERAL RESERVE SYSTEM

The Federal Reserve System is the central bank of the United States. It performs five key functions to promote the effective operation of the U.S. economy and, more generally, the public interest.

The Federal Reserve

- **conducts the nation's monetary policy** to promote maximum employment and stable prices in the U.S. economy;
- **promotes the stability of the financial system** and seeks to minimize and contain systemic risks through active monitoring and engagement in the U.S. and abroad;
- **promotes the safety and soundness of individual financial institutions** and monitors their impact on the financial system as a whole;
- **fosters payment and settlement system safety and efficiency** through services to the banking industry and U.S. government that facilitate U.S.-dollar transactions and payments; and
- **promotes consumer protection and community development** through consumer-focused supervision and examination, research and analysis of emerging consumer issues and trends, community economic development activities, and administration of consumer laws and regulations.

To learn more about us, visit www.federalreserve.gov/aboutthefed.htm.

Contents

Overview

The Consolidated Appropriations Act, 2021[1] (CAA) requires the Board of Governors of the Federal Reserve System (Board) to submit annually for seven years a report focused on cybersecurity to Congress. The CAA calls for a description of measures the Board has undertaken to strengthen cybersecurity within the financial services sector and with respect to the Board's functions as a regulator, including the supervision and regulation of financial institutions and third-party service providers. Pursuant to the CAA, this report is organized in three main sections covering:

- the Board's policies and procedures related to cybersecurity risk management, including with respect to the Board's supervision and regulation of financial institutions, the Board's administration of its internal information security program, and the Reserve Banks' information security program;
- Board activities to address cybersecurity risks, including those carried out through our supervision of financial institutions, through the Board's own programs and initiatives, and through those of the Reserve Banks as a provider of critical payment and settlement services; and
- current and emerging cyberthreats that may pose a risk to the resilience of the financial system.

As described in the report, the Board views cybersecurity as a high priority for the Federal Reserve System (System) and Board-supervised institutions. The Board and the Reserve Banks maintain robust information security programs and engage and coordinate on cybersecurity issues with numerous critical stakeholders including the financial regulatory agencies and industry. These efforts include actively monitoring cybersecurity threats and responding, as appropriate, to incidents that could affect the operations of the Board, the Reserve Banks, or supervised institutions.

[1] Consolidated Appropriations Act, Pub. L. No. 116-260, Division Q, section 108 (2021).

Board Policies and Procedures for Cybersecurity Risk Management

The Board recognizes the increasing and evolving nature of cybersecurity threats to the financial system. Accordingly, the Board's supervision and regulation of financial institutions encompasses review and monitoring of institutions' cybersecurity risk management and information technology (IT) programs. As part of its safety and soundness supervision, the Board issues cybersecurity-related regulations and guidance, examines and monitors supervised institutions' cybersecurity risk-management posture, and collects data on cyber incidents (along with the other federal financial regulatory agencies) to monitor trends in the financial services sector. Additionally, the Board and the Reserve Banks secure their internal information and information systems through robust cybersecurity risk-management programs. The Board follows the Federal Information Security Modernization Act (FISMA) requirements, and the Reserve Banks also employ a framework based on the National Institute of Standards and Technology's (NIST) standards and guidance.

Board Supervisory Policies and Procedures

The Board's supervisory policies and examination procedures are aimed at reducing the risk of cybersecurity threats to the financial system through effective cybersecurity practices at supervised institutions. The Board issues and publishes rules and guidance for supervised institutions regarding IT risk management, cybersecurity, operational resilience, third-party risk management, and other related topics.[2]

The Board and other regulatory agencies also publish interagency guidance on various aspects of information security risk within the financial services sector. For example, the Interagency Guidelines Establishing Information Security Standards impose requirements on banking organizations to develop and implement administrative, technical, and physical safeguards to promote the security, confidentiality, and integrity of customer information.[3]

In addition, the Board utilizes general safety and soundness guidelines to mitigate cyber risk.[4] These guidelines require banks to have internal controls and information systems appropriate to

---

[2] See Board of Governors of the Federal Reserve System, "Information Technology Guidance," last modified February 4, 2022, https://www.federalreserve.gov/supervisionreg/topics/information-technology-guidance.htm and Board of Governors of the Federal Reserve System, "Operational Resilience," last modified February 4, 2022, https://www.federalreserve.gov/supervisionreg/topics/operational-resilience.htm.

[3] See 12 C.F.R. pt. 208, appendix D-2; 12 C.F.R. pt. 225, appendix F. These requirements of banking organizations are pursuant to title V, subtitle A, of the Gramm-Leach-Bliley Act.

[4] See Interagency Guidelines Establishing Standards for Safety and Soundness Standards, 12 C.F.R. pt. 30, appendix A (proposed July 10, 1995).

the size of the institution and to the nature, scope, and risk of its activities and that provide for, among other requirements, effective risk assessment and adequate procedures to safeguard and manage assets. The safety and soundness standards also require banks to have internal audit systems that provide for adequate testing and review of information systems.

Further, the Board's domestic regulatory, supervisory, and oversight framework for financial market infrastructures (FMIs) consists of the Board's Regulation HH and part I of the Federal Reserve Policy on Payment System Risk (PSR policy). Regulation HH imposes risk-management standards on "financial market utilities" (FMUs)[5] that the Financial Stability Oversight Council has designated as systemically important under title VIII of the Dodd-Frank Wall Street Reform and Consumer Protection Act (Dodd-Frank Act title VIII).[6] Part I of the PSR policy sets out risk-management standards for certain FMIs that are not subject to Regulation HH, including payment and settlement systems operated by the Reserve Banks. The risk-management standards in Regulation HH and the PSR Policy reflect the relevant international standards for these FMIs—the *Principles for Financial Market Infrastructures*, or PFMI issued by the Committee on Payments and Market Infrastructures and the International Organization of Security Commissions (CPMI-IOSCO).[7] Several of these standards are relevant to the management and mitigation of cyber risk, including standards related to governance, operational risk (including cybersecurity risks), and comprehensive risk management.

The Board's FMI supervisory teams also utilize other relevant cybersecurity risk guidance, such as the CPMI-IOSCO's *Guidance on Cyber Resilience for Financial Market Infrastructures* (Cyber Resilience Guidance),[8] to supplement the PFMI operational risk-management expectations. Additionally, following a rise in incidents where threat actors exposed weak cybersecurity practices at firms that participate in FMIs, the CPMI published a strategy on reducing the risk of wholesale payments fraud related to endpoint security.

See table 1 for recent Board actions and actions in collaboration with other financial regulatory agencies to promote cybersecurity.

---

[5] The term *FMU* is defined under title VIII and generally refers to payment, clearing, and settlement systems. The term *FMI* is used internationally. FMUs are a subset of FMIs—in particular, the term FMI includes trade repositories while the term FMU does not.

[6] See 12 C.F.R. pt. 234. The risk-management standards in Regulation HH apply to designated FMUs for which the Board is the lead supervisory agency, while comparable CFTC and SEC regulations apply to other designated FMUs.

[7] See Committee on Payment and Settlement Systems and Technical Committee of the International Organization of Securities Commissions, *Principles for Financial Market Infrastructures* (Basel: Bank for International Settlements, April 2012), https://www.bis.org/cpmi/publ/d101a.pdf. *Principles for Financial Market Infrastructures* and subsequent supplemental guidance documents were issued by the international standard-setting bodies for FMIs: the Committee on Payments and Market Infrastructures of the Bank for International Settlements and the International Organization of Securities Commissions (CPMI-IOSCO).

[8] See Committee on Payments and Market Infrastructures and the Board of the International Organization of Securities Commissions (IOSCO), Guidance on Cyber Resilience for Financial Market Infrastructures (Basel: Bank for International Settlements, June 2016), https://www.bis.org/cpmi/publ/d146.htm.

Table 1. Recent Board and interagency actions to promote cybersecurity

Date	Action
October 3, 2022	The Board, together with the other members of the Federal Financial Institutions Examination Council (FFIEC), published an updated Cybersecurity Resource Guide for Financial Institutions in October 2022. The purpose of this guide is to help financial institutions prepare and respond to cyber incidents. The resource guide includes updated references and specific resources to address the ongoing threat of ransomware incidents.[1]
October 5, 2022	The Board invited comment on updates to operational risk-management requirements for certain systemically important financial market utilities (FMUs) supervised by the Board. FMUs provide essential infrastructure to clear and settle payments and other financial transactions upon which the financial markets and the broader economy rely to function effectively. The proposal would update, refine, and add specificity to the operational risk management requirements in Regulation HH to reflect changes in the operational risk, technology, and regulatory landscapes in which designated FMUs operate since the Board last amended this regulation in 2014. The proposal would also adopt specific incident-notification requirements.[2]
June 6, 2023	The Board, together with the Federal Deposit Insurance Corporation (FDIC) and the Office of the Comptroller of the Currency (OCC), issued final joint guidance designed to help banking organizations manage risks associated with third-party relationships. The final guidance • describes principles and considerations for banking organizations' risk management of third-party relationships, including key considerations for cybersecurity and operational risks associated with such relationships; • emphasizes that sound third-party risk management considers the level of risk, complexity, and size of the banking organization, as well as the nature of each third-party relationship; and • offers a framework with illustrative examples covering various stages in the life cycle of third-party relationships. Banking organizations can use these examples to align their risk management practices with the nature and risk profile of their third-party relationships.[3]

[1] See "Cybersecurity Resource Guide for Financial Institutions," Federal Financial Institutions Examination Council, last updated September 2022, https://www.ffiec.gov/press/pdf/FFIECCybersecurityResourceGuide2022ApprovedRev.pdf.

[2] See Financial Market Utilities, 87 Fed. Reg. 60314 (proposed October 5, 2022), https://www.federalregister.gov/documents/2022/10/05/2022-21222/financial-market-utilities.

[3] See "Agencies Issue Final Guidance on Third-Party Risk Management," June 6, 2023, https://www.federalreserve.gov/newsevents/pressreleases/bcreg20230606a.htm

Board Internal Policies and Procedures

The Board has taken a proactive approach to safeguarding its operations and assets by developing, documenting, and implementing a comprehensive security program. The program is designed to protect both the information and information systems that support the agency's core mission functions. The Board's information security program follows federal information security requirements as established by FISMA and related NIST standards.

In accordance with the President's "Executive Order on Improving the Nation's Cybersecurity,"[9] the Board is taking steps to further improve its security posture by implementing the latest cybersecurity standards and principles. A key area of focus is the adoption of zero trust principles,[10] which are representative of a security framework requiring all users, whether inside or outside the organization's network, to be authenticated, authorized, and continuously validated before accessing applications and data and which will further enhance the Board's cybersecurity posture.

The Board's Office of Inspector General (OIG) performs independent and regular assessments of the agency's security programs, practices, and systems. Furthermore, the Board also collaborates with cybersecurity consultants and experts, who provide independent recommendations on improving the Board's cybersecurity controls and protocols.

In addition to administering the agency's information security program, the Board also oversees the cyber-risk management posture of the Reserve Banks. The Reserve Banks have a comprehensive, risk-based information security program that is informed by NIST standards and guidance and industry best practices. The Reserve Banks, as operators of critical financial services, proactively provide tools and communications aimed at mitigating cyber risks to their financial institution customers. Additionally, Federal Reserve Operating Circular No. 5, Electronic Access sets forth the information security requirements applicable to institutions accessing Reserve Bank services, such as the Fedwire Funds Service, the Fedwire Securities Service, FedACH, and the National Settlement Service.[11] Under Operating Circular No. 5, institutions are required to implement technical, operational, managerial, and procedural controls designed to protect the security of the IT environment, including systems and processes that are used to access Reserve Bank services and applications.

---

[9] See The White House, "Executive Order on Improving the Nation's Cybersecurity," last modified on May 12, 2021, https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/.

[10] See OMB, M-22-09, Moving the U.S. Government Toward Zero Trust Cybersecurity Principles, January 26, 2022, https://www.whitehouse.gov/wp-content/uploads/2022/01/M-22-09.pdf.

[11] See "Federal Reserve Banks Operating Circular No. 5 Electronic Access," effective June 30, 2021, https://www.frbservices.org/binaries/content/assets/crsocms/resources/rules-regulations/101520-operating-circular-5.pdf.

Board Activities to Address Cybersecurity Risks

The Board's activities help ensure the policies, procedures, rules, and guidance for supervised institutions and internal agency functions are successfully implemented. The Board's approach includes ensuring appropriate staffing, training, and resources for bank examiners. The Board OIG also evaluates cybersecurity supervisory activities and enhancements to the Board's internal processes. The Board's activities involve interagency, intergovernmental, industry, and international collaboration.

Supervisory Activities

The Federal Reserve conducts examinations and monitoring of cybersecurity risk management, governance, and controls at supervised institutions. It also examines and monitors, pursuant to the Board's authority under the Bank Service Company Act (BSCA),[12] certain services performed on behalf of financial institutions by their service providers. The Federal Reserve's supervision activities in this area promote financial institutions' ability to protect against cyber incidents and other hazards, safeguard critical infrastructure, and address emerging technology risks. The Federal Reserve examination staff uses the Uniform Rating System for Information Technology (URSIT) and the *FFIEC IT Handbook*, which is informed by NIST standards and guidance along with other sources, in conducting cybersecurity and other IT-related examinations.

Examiners evaluate cybersecurity with consideration of the business model and activities conducted by supervised institutions as part of a principles-based supervision program. The scope of examinations considers key cybersecurity risks, the industry landscape, and other factors such as emerging technologies. As part of these evaluations, examiners consider business-line controls, risk-management practices, assurance functions, and governance activities performed by the firms' senior management and board of directors.

For the eight U.S. global systemically important banks, the Federal Reserve conducts joint cybersecurity examinations or coordinated cyber reviews with the OCC and FDIC. Additionally, for large financial institutions with assets of $100 billion or more,[13] the Federal Reserve conducts hori-

[12] 12 U.S.C. §§ 1861-67.

[13] A LISCC firm is a firm that is supervised under the Large Institution Supervision Coordinating Committee supervisory program. Current LISCC firms are Bank of America Corporation; The Bank of New York Mellon Corporation; Citigroup, Inc.; The Goldman Sachs Group, Inc.; JPMorgan Chase & Co.; Morgan Stanley; State Street Corporation; and Wells Fargo & Company. An LFBO firm refers to a domestic or foreign banking organization with combined U.S. assets of $100 billion or more that is supervised under the Large and Foreign Banking Organization supervisory program.

zontal cybersecurity examinations across institutions. Horizontal examinations promote consistency in the assessment of cyber governance and controls across firms, establish range of practice, and, as appropriate, allow the Federal Reserve to issue supervisory findings when weaknesses are present. In addition to the horizontal reviews, supervisory teams monitor cyber, IT, and operational risk using continuous monitoring processes as well as monthly engagement focused on emerging threats.

For community banking organizations (those with under $10 billion in assets) and regional banking organizations (those with $10 to $100 billion in assets), URSIT is the primary mechanism to evaluate cybersecurity. If deficiencies in an institution's cybersecurity program are identified, examiners may issue supervisory findings. Firms are expected to promptly address findings to ensure appropriate protection against cyberthreats.

For community banking organizations and regional banking organizations, the Board uses a risk-focused approach that assigns examination resources to higher-risk areas of each bank's operations and ensures that banks maintain risk-management capabilities appropriate to their size and complexity. Cybersecurity practices are evaluated with standardized procedures through regular IT examinations. For state member banks, these examinations are often conducted jointly with state banking regulators. The Federal Reserve along with the FDIC and state banking authorities use the Information Technology Risk Examination Program, which provides supervisory staff with risk-focused and efficient examination procedures for assessing IT and cybersecurity risks at supervised institutions.

The Federal Reserve expects financial institutions to effectively manage risks associated with their third-party service providers. Additionally, the BSCA provides authority for the federal banking agencies (FBAs)[14] to regulate and examine certain services performed by third parties on behalf of insured depository institutions and their affiliates. The FBAs jointly supervise a subset of third-party technology service providers through an interagency technology service provider supervision program, which incorporates a risk-based process for selecting service providers included in the program. Through examinations of service providers in the program, the agencies issue an URSIT rating evaluating the service provider. As part of the examinations, the agencies conduct cybersecurity-specific examinations of these service providers which informs the firm's overall URSIT rating. The agencies issue reports of examination, communicate supervisory findings, and take enforcement actions when needed. The report of examination is distributed on a confidential basis to the service provider and to the provider's client financial institutions to assist with their ongoing monitoring of third-party risk.

[14] The federal banking agencies are the Federal Reserve Board (Board), Office of the Comptroller of the Currency (OCC), and Federal Deposit Insurance Corporation (FDIC).

In addition, the Federal Reserve's consumer compliance supervision program complements the IT and cybersecurity reviews conducted by safety and soundness examiners to ensure that supervised institutions maintain systems and processes to protect customers' sensitive personal financial information. Through this program, the Federal Reserve's examiners evaluate the effectiveness of supervised institutions' compliance with consumer financial privacy laws and regulations.[15]

For the FMU portfolio, the Board has direct supervisory authority for a subset of the designated FMUs and works closely with staff at the New York and Chicago Reserve Banks, as well as at the Commodity Futures Trading Commission (CFTC) and Securities and Exchange Commission (SEC), to supervise the other designated FMUs. Specific focus is placed on FMUs' operational and cyber-risk management programs.[16] The Board regularly sets supervisory priorities for and examines (and participates in CFTC- and SEC-led examinations of) designated FMUs' operational risk-management frameworks.[17] The Board also reviews proposed changes to designated FMUs' rules, procedures, and operations, including proposed changes that would materially affect a designated FMU's operational and cyber-risk management. Several PFMI standards that address cyber risk (including standards related to governance, operational risk, and comprehensive risk management), as well as the Cyber Resilience Guidance, provide common reference points for the three regulatory agencies in their supervision and oversight of the designated FMUs.

The Federal Reserve uses the ORSOM (Organization, Risk Management, Settlement, Operational Risk and Information Technology, and Market Support, Access, and Transparency) rating system in its assessment of designated FMUs. The rating system facilitates discussion of the FMU's condition with the FMU's management and board of directors. For a designated FMU for which the Board is the supervisory agency under title VIII of the Dodd-Frank Act, supervisory staff explain to the FMU the factors that determine that FMU's rating, including operational risks and IT, which covers cyber risk.[18]

Furthermore, as part of our supervisory activities, the Federal Reserve has established processes and programs to monitor and share information involving cybersecurity threats, vulnerabilities, and incidents across the System. Additionally, the Federal Reserve monitors cybersecurity developments and events across the financial services sector including the payment, clearing, and settlement systems. The Federal Reserve proactively alerts examination staff to imminent cyberthreats or vulnerabilities including ransomware, malware, and distributed denial of service (DDoS)

---

[15] Examples include Regulation P (12 C.F.R. pt. 1016.) and the "red flags" rule under the Fair Credit Reporting Act (15 U.S.C. § 1681m(e)).

[16] See Board of Governors of the Federal Reserve System, "Designated Financial Market Utilities," last modified January 29, 2015, https://www.federalreserve.gov/paymentsystems/designated_fmu_about.htm.

[17] Under section 807(d) of the Dodd-Frank Act, the Board may, at its discretion, participate in any title VIII examination led by the SEC or CFTC. 12 U.S.C § 5466)(d)(2).

[18] For designated FMUs that are primarily supervised by the CFTC or SEC, Federal Reserve supervisory staff communicate assessments of the FMU's cyber-risk management to the CFTC or SEC, as appropriate.

impacting the financial sector. These notifications provide examination staff the context to proceed with the appropriate Federal Reserve supervisory actions.

The Board and other FBAs require a banking organization to notify its primary regulator of computer-security incidents that rise to the level of a notification incident within 36 hours of determining that such an incident has occurred. A bank service provider is required to notify affected banking organization customers as soon as possible regarding certain computer-security incidents so the customer banking organizations can determine whether a notification incident has occurred. The notifications help the agencies become aware of and react to emerging threats, as well as enable the Board to assist affected institutions, including community banks who may face a greater challenge in responding to such an incident.[19] In the proposed revisions to Regulation HH, a designated FMU would need to notify affected participants immediately in the event of actual disruptions or material degradation to its critical operations or services or to its ability to fulfill its obligations on time. In addition, a designated FMU would need to notify all participants and other relevant entities in a timely and responsible manner of all other material operational incidents that require immediate notification to the Board.[20]

Cybersecurity-Related Findings

As part of the Board's safety and soundness supervision, Federal Reserve supervisors examine and monitor the information security practices and cybersecurity programs of supervised institutions and may issue supervisory findings notifying supervised institutions of identified deficiencies. The Federal Reserve requires supervised institutions to respond appropriately to cybersecurity-related supervisory findings and take proactive steps to mitigate cyber risk. When institutions do not address findings in an appropriate period of time, the Board has tools such as informal and formal enforcement actions to ensure institutions operate in a safe and sound manner. The Board has observed improvement in cybersecurity practices over the past several years resulting from supervised institutions' efforts to address supervisory findings as well as proactive steps taken by the institutions.

Staffing, Training, and Deployment of Examiner Resources

The Federal Reserve maintains an experienced, trained complement of supervision staff with IT expertise, including individuals with expertise in cybersecurity. Federal Reserve examiners assess supervised institutions' cyber and information security practices, internal audit, risk management, and controls to ensure that institutions implement appropriate and effective safeguards to

[19] See Board of Governors of the Federal Reserve System, "Contact Information in Relation to Computer-Security Incident Notification Requirements," SR letter 22-4 (March 29, 2022), https://www.federalreserve.gov/supervisionreg/srletters/SR2204.htm.

[20] See Financial Market Utilities, 87 Fed. Reg. 60314 (proposed October 5, 2022), https://www.federalregister.gov/documents/2022/10/05/2022-21222/financial-market-utilities.

mitigate cyber risk. For large domestic firms and service providers, using a risk-based approach, examiners are assigned to a specific firm or group of firms, and for foreign entities and smaller domestic institutions, examiners are assigned on a portfolio basis.

The Federal Reserve has established frameworks to direct the recruitment, hiring, and assignment of examiners, including IT and cybersecurity risk specialists. The Federal Reserve conducts training to ensure examiners remain prepared to address the latest threats to the financial services sector and regularly updates its training program to ensure readiness to address current and prospective threats. The Federal Reserve makes available to all staff an online and mobile learning platform with an extensive catalogue of IT and information security training. The Federal Reserve continues to assess and offer cyber skills training needs aligned with risks to supervised institutions. In addition, Federal Reserve examiners frequently participate in conferences and training events to gain perspective from external cybersecurity practitioners. Affinity groups at the Federal Reserve serve as useful forums to share information and institutional knowledge of cyber resilience issues, including committees that address operational resilience matters across the portfolios supervised by the Federal Reserve. We also leverage FFIEC trainings, conferences, and tools for examiners.

Board OIG Efforts Related to Supervisory Activities

The OIG issued a report, *Results of Scoping the Evaluation of the Board and Reserve Banks' Cybersecurity Incident Response Process for Supervised Institutions*, on June 26, 2023, which identified findings and recommendations to improve the effectiveness of the cybersecurity incident response process. In this report, the OIG recommends that the Board update the cybersecurity incident response process's mission and governance structure and enhance guidance and training to improve effectiveness. [21] The Board is taking measures to address the OIG's recommendations.

In 2020, the OIG issued a report identifying opportunities for the Board to enhance cybersecurity supervision of LISCC firms related to governance, ratings, and training.[22] The Board successfully addressed the areas needing improvement. As of September 2022, all recommendations from this report were closed by the OIG.

In 2017, the OIG conducted an evaluation to assess the Board's cybersecurity examination approach and to determine whether the Board was providing effective oversight of supervised

[21] See Board of Governors of the Federal Reserve System, Office of Inspector General, *Results of Scoping of the Evaluation of the Board and Reserve Banks' Cybersecurity Incident Response Process for Supervised Institutions* (Washington: Board of Governors, June 2023), https://oig.federalreserve.gov/reports/board-cyber-incident-response-jun2023.pdf.

[22] See Board of Governors of the Federal Reserve System, Office of Inspector General, *The Board's Approach to the Cybersecurity Supervision of LISCC Firms Continues to Evolve and Can Be Enhanced* (Washington: Board of Governors, September 2020), https://oig.federalreserve.gov/reports/board-cybersecurity-supervision-LISCC-firms-sept2020.htm.

institutions' information security controls and cybersecurity risk for select oversight areas.[23] The Board successfully addressed all areas and all recommendations except for one, where the OIG had recommended that the Board reiterate to financial institutions the requirement under the BSCA to notify their primary regulator of the existence of new service relationships. The Board has evaluated options and is coordinating with other FBAs to clarify, reiterate, and improve compliance with this requirement.

Reserve Bank Activities

In addition to administering the Board's internal information security program, the Board also supervises the Reserve Banks' IT operations. The Reserve Banks continue to take measures to ensure they have robust protective measures for their critical operations. The Reserve Banks remain vigilant about their cybersecurity posture, investing in risk-mitigation initiatives and programs and continuously monitoring and assessing cybersecurity risks to operations and protecting systems and data. For example, the Reserve Banks' overall security posture continues to be strengthened through several high-priority cybersecurity initiatives, including enhancements to identity and access management capabilities, increased efforts to mitigate risks posed by vendors and service providers, and a focus on aligning with the pillars of zero trust architecture. Additionally, in light of ongoing ransomware activity in the financial sector, the Reserve Banks continue to take actions to strengthen processes, infrastructure, and controls to further enhance ransomware protections and response capabilities consistent with the Cybersecurity and Infrastructure Security Agency (CISA) and Federal Bureau of Investigation (FBI) guidance on mitigating ransomware risks.

The Reserve Banks have also focused their efforts on bolstering the security of the U.S. payment system. This includes enhancing the resiliency and information security posture of Federal Reserve Financial Services through efforts to improve recovery capabilities. Additionally, the Reserve Banks maintain an information security program for FedLine Solutions, which provides financial institutions direct electronic access to the Reserve Banks' payment services.[24] As part of this program, financial institutions that use FedLine Solutions must conduct an annual assessment of their compliance with the Reserve Banks' FedLine security requirements and submit an attestation that they have completed the assessment. To the extent any deficiencies or gaps are identified in the self-assessment, institutions must develop a remediation plan to address such deficiencies.

Finally, the Reserve Banks continue to monitor cybersecurity legislation and executive orders focused on cybersecurity and resiliency. This includes working with the Board to track progress of CISA's incident reporting rule under the Cyber Incident Reporting for Critical Infrastructure Act.

---

[23] See Board of Governors of the Federal Reserve System, Office of Inspector General, *The Board Can Enhance Its Cybersecurity Supervision Approach in the Areas of Third-Party Service Provider Oversight, Resource Management, and Information Sharing* (Washington: Board of Governors, April 2017), https://oig.federalreserve.gov/reports/board-cybersecurity-supervision-apr2017.htm.

[24] See "Assurance Program Frequently Asked Questions," Federal Reserve Bank Services, https://www.frbservices.org/resources/fedline-solutions/faq/fedline-assurance-program.html.

Through these efforts, the Reserve Banks work together and with government partners to further enhance the state of information security and resiliency across the System.

Coordination Activities

Due to the high degree of interconnectedness of the global financial system, the Board is an active participant and leader in domestic and international forums addressing the cyber resiliency of the financial services sector. The Board closely coordinates with other domestic and international agencies, governance bodies, financial regulators, and industry to share information and best practices as well as publish guidance for regulated entities.

Intergovernmental Coordination

To strengthen risk-management practices across the financial services sector and reduce the effects of cyber-related incidents, the Board coordinates with partners through the President's Working Group on Financial Markets (PWGFM), the Financial and Banking Information Infrastructure Committee (FBIIC), and the Federal Financial Institutions Examination Council (FFIEC).

The Board is a member of the PWGFM, whose mission is to enhance the integrity, efficiency, orderliness, and competitiveness of the nation's financial markets and their ability to maintain investor confidence. A significant part of this mission is related to cyber and other operational risks. Most recently, the Board has actively contributed to the group's initiatives related to cyber incident communications.

The Board is also a member of the FBIIC, which is chartered under the PWGFM. FBIIC is composed of federal and state financial regulatory agencies that supervise banking, investment, and insurance firms, and is chaired by the U.S. Department of the Treasury (Treasury). FBIIC members engage in efforts to strengthen the security and resiliency of critical infrastructure across the financial services sector, including financial institutions regulated and supervised by the FBIIC member organizations. In the past year, FBIIC has engaged on a number of areas relating to cybersecurity, cloud adoption, data protection, and incident response. For example, experts from the Federal Reserve assisted the Treasury with developing a report exploring how the use of cloud services may affect the sector's operational resilience and incident response.[25]

The Board participates in FBIIC's periodic cyber exercises that include participation from the regulatory agencies, financial institutions, and trade associations. These exercises have proved useful in advancing incident management and information sharing protocols across the financial services sector. Additionally, through participation in these exercises, the Board has improved its ability to respond to, in coordination with other financial regulators, potential operational disruptions in the

[25] See U.S. Department of the Treasury, *The Financial Services Sector's Adoption of Cloud Services* (Washington: Department of the Treasury, 2023), https://home.treasury.gov/system/files/136/Treasury-Cloud-Report.pdf.

financial services sector's critical infrastructure. These exercises also have led to the creation of private sector-led and public sector-supported initiatives to enhance cyber resiliency. These include an initiative to enable participating financial institutions to store critical customer account data in a secure industry-standard format, and capabilities to proactively identify, analyze, and coordinate activities to mitigate systemic risk to the U.S. financial system (and other critical infrastructure) from cyberthreats.

In addition, as a member of the FFIEC, which is an interagency body that promotes uniformity and consistency in the examination of financial institutions across its members, the Board actively coordinates with FFIEC members on cybersecurity risk-management issues. The Board contributes to the efforts of the FFIEC in responding to cyber incidents affecting institutions supervised by FFIEC members. The Board also contributes to the FFIEC's efforts and supports ongoing dialogue on cybersecurity issues and opportunities to improve consistency in examination approaches.

- In August 2022, the FFIEC IT Subcommittee sponsored its annual IT Conference for examiners that highlighted current and emerging technology issues affecting supervised institutions including cybersecurity attack techniques and impacts from geopolitical events, ransomware response, artificial intelligence or machine learning threat detection and bias prevention, and banking as a service. The conference was attended by more than 530 examiners from federal and state regulatory agencies.
- In recognition of National Critical Infrastructure Security and Resilience Month, on November 18, 2022, the Cybersecurity and Critical Infrastructure Subcommittee (CCIS) hosted an Industry Outreach webinar focusing on multifactor authentication (MFA). During the event, representatives from FinCEN and CCIS discussed operational resilience and the use of MFA, including related decisionmaking and FFIEC guidance.
- Throughout 2022, the CCIS issued timely messages on significant cybersecurity issues and information to supervised institutions. These communications heightened awareness on the CISA "Shields-Up" initiative to promote awareness of current cybersecurity threats and mitigations; the joint Cybersecurity Advisory on Understanding and Mitigating Russian State-Sponsored Cyberthreats to U.S. Critical Infrastructure by CISA, FBI, and National Security Agency; and the availability of the Treasury's Office of Cybersecurity and Critical Infrastructure Protection monthly unclassified threats exchange.

The Board continues to follow the ongoing developments with the NIST Cybersecurity Framework (CSF). The CSF 2.0 update aims to keep pace with the evolving cybersecurity landscape and helps banking organizations strengthen cyber-risk management and reduce those risks with customized measures. Banks that adopt a standardized approach are better able to track their progress over

time and share information and best practices with other financial institutions and regulators.[26] Additionally, the Board coordinates through the Cybersecurity Forum for Independent and Executive Branch Regulators and monitors various CISA initiatives (e.g., Cyber Incident Reporting for Critical Infrastructure Act).

Public and Private Sector Coordination

The Board participates in various industry-led initiatives to enhance cybersecurity risk management. For example, the Board is a member of the Financial Services Information Sharing and Analysis Center (FS-ISAC), the global financial industry's resource for cyber and physical threat intelligence analysis and sharing. The Board encourages its supervised institutions to incorporate threat monitoring programs and participate in information sharing organizations such as the FS-ISAC.

Through FBIIC, the Board also coordinates with the Financial Services Sector Coordinating Council (FSSCC), a nonprofit body composed of more than 70 members from across the financial services industry whose mission is to strengthen the resiliency of the financial services sector. This partnership focuses on improving the financial services sector's ability to rapidly respond to and recover from significant cybersecurity incidents, thereby reducing the potential for such incidents to threaten the stability of the financial system and the broader economy. In 2022, joint FBIIC and FSSCC priorities included the protection of supervisory data, cyber exercises, and cyber workforce development.

One important example of this type of coordination is the "Hamilton Series." For this initiative, the Treasury partners with the Board, other U.S. government agencies, the FSSCC, and FS-ISAC to develop cyber exercises aimed at improving responses to a range of cyberthreat scenarios within the U.S. financial sector. These cyber exercises serve to better prepare the financial sector and the public sector response to cyberattacks.

International Coordination

The Board leads or contributes to cybersecurity activities undertaken by groups such as the Financial Stability Board (FSB), the Basel Committee on Banking Supervision (BCBS), the Committee on Payment and Market Infrastructures (CPMI) (and its joint efforts with the International Organization of Securities Commissions (IOSCO)), the International Association of Insurance Supervisors (IAIS), and the Group of Seven (G7).

In light of the threats cyber incidents pose to the interconnected global financial system, the FSB has assumed a key role in promoting cyber resilience. The Board contributed to the FSB's work aimed to promote greater convergence in cyber incident reporting in three ways:

[26] Federal Financial Institutions Examination Council, "FFIEC Encourages Standardized Approach to Assessing Cybersecurity Preparedness," news release, August 28, 2019, https://www.ffiec.gov/press/pr082819.htm.

- setting out recommendations to address the issues identified as impediments to achieving greater harmonization in cyber incident reporting[27]
- enhancing the FSB's Cyber Lexicon to include additional terms related to cyber incident reporting[28]
- developing a concept for a common format for incident reporting exchange (FIRE) to collect incident information from financial institutions and between themselves, published April 13, 2023[29]

In addition, the FSB continues its work to enable the financial system to adapt to structural changes in relation to strengthening financial institutions' ability to manage third-party and outsourcing risk.[30]

The BCBS acts as the primary global standard setter for the prudential regulation of banks and provides a forum for cooperation on banking supervisory matters. The Board's deputy director of Supervision and Regulation currently serves as the chair of the BCBS Operational Resilience Group (ORG). In March 2021, the BCBS issued the Principles for Operational Resilience[31] and the Principles for the Sound Management of Operational Risk, which the ORG was charged with drafting.[32] These documents highlight the importance of sound operational risk management, including cyber-risk management, and are aligned with guidance released by the Board on operational resilience.[33] In September 2021, the BCBS published a newsletter calling for increased efforts to improve banks' resilience to cyberthreats, intended to complement earlier actions and promote widespread adoption of measures to strengthen banks' cybersecurity.[34]

Through the CPMI-IOSCO, the Board has played a key role in the development of the PFMI and related guidance for FMIs, including the Cyber Resilience Guidance. The CPMI-IOSCO Working Group on Cyber Resilience has promoted implementation of the guidance across member jurisdic-

---

[27] See Financial Stability Board, *Recommendations to Achieve Greater Convergence in Cyber Incident Reporting: Final Report*, (Basel: Financial Stability Board, April 2023), https://www.fsb.org/wp-content/uploads/P130423-1.pdf.

[28] See "Cyber Lexicon," Financial Stability Board, last modified April 2023, https://www.fsb.org/wp-content/uploads/P130423-3.pdf.

[29] See "Format for Incident Reporting Exchange (FIRE): A possible way forward," Financial Stability Board, last modified on April 13, 2023, https://www.fsb.org/wp-content/uploads/P130423-2.pdf.

[30] See Financial Stability Board, "Enhancing Third-Party Risk Management and Oversight," Discussion Paper (Basel: Financial Stability Board, June 2023), https://www.fsb.org/wp-content/uploads/P220623.pdf.

[31] See Basel Committee on Banking Supervision, *Principles for Operational Resilience* (Basel: Bank for International Settlements, March 2021), https://www.bis.org/bcbs/publ/d516.pdf.

[32] See Basel Committee on Banking Supervision, *Revisions to the Principles for the Sound Management of Operational Risk* (Basel: Bank for International Settlements, March 2021), https://www.bis.org/bcbs/publ/d515.pdf.

[33] See Board of Governors of the Federal Reserve System, "Interagency Paper on Sound Practices to Strengthen Operational Resilience," SR letter 20-24 (November 2, 2020), https://www.federalreserve.gov/supervisionreg/srletters/SR2024.htm.

[34] See Bank for International Settlements, "Basel Committee Calls for Improved Cyber Resilience, Reviews Climate-Related Financial Risks and Discusses Impact of Digitalization," news release, September 20, 2021, https://www.bis.org/press/p210920a.htm.

tions and engaged with private sector firms to better understand operational risks and cybersecurity risk management.

The Board contributed to the development of IAIS's key financial stability priorities for insurance providers in November 2021. Among these was a focus on growing cyber risks, which is increasingly creating significant impacts to insurers' financial liabilities. In 2021, the Board contributed to the first full global monitoring exercise conducted by the IAIS to assess global insurance market trends and developments and detect the possible build-up of systemic risk in the global insurance sector, including heightened cyber risk.[35]

Given the rapidly evolving nature of cyber risks and the cross-border and cross-sector relevance of cyberthreats, the G7 finance ministers, central bank governors, and other financial authorities coordinate through a working group consisting of cybersecurity experts to elevate cybersecurity concerns and enhance cooperation among G7 jurisdictions and the financial services sector. The G7 Cyber Expert Group has published papers on cybersecurity topics, including a paper calling for common categorizations of malicious cyber incidents and other operational IT incidents to aid in comparing and studying incidents across jurisdictions.[36] Current G7 cyber priorities include coordinating responses to ransomware, cyber events across jurisdictions, and cyber risks from third-party service providers and emerging technologies. In 2022, the Board, as part of the G7 Cyber Expert Group published two reports addressing ransomware and third-party risk within the financial sector:

- *G7 Fundamental Elements of Ransomware Resilience for the Financial Sector* provides financial entities with high-level building blocks for addressing ransomware threats. The aim of this document is to assist financial institutions and authorities in implementing their own internal ransomware mitigation activities and promoting greater ransomware resilience across the entire financial sector.[37]
- *G7 Fundamental Elements for Third-Party Cyber-Risk Management in the Financial Sector* is an update to a previous version published in 2018.[38] The G7 deemed this update necessary to keep pace with the ever-changing cyberthreat landscape, particularly vulnerabilities resulting from financial institutions' increasing use of service providers in central operational functions.

---

[35] See International Association of Insurance Providers, "IAIS Global Monitoring Exercise (GME) Highlights Key Financial Stability Priorities for Insurance Supervisors," news release, November 30, 2021, https://www.iaisweb.org/uploads/2022/01/211130-IAIS-Press-Release-GIMAR-2021.pdf.

[36] See Cyber Expert Group, "Proposal for a Common Categorization of IT Incidents," April 6, 2021, https://www.bancaditalia.it/pubblicazioni/mercati-infrastrutture-e-sistemi-di-pagamento/approfondimenti/2021-006/index.html?com.dotmarketing.htmlpage.language=1&dotcache=refresh&dotcache=refresh.

[37] See "G7 Fundamental Elements of Ransomware Resilience for the Financial Sector," October 2022, https://home.treasury.gov/system/files/216/G7-FUNDAMENTAL-ELEMENTS-OF-RANSOMWARE-RESILIENCE-FOR-THE-FINANCIAL-SECTOR.pdf.

[38] See "G7 Fundamental Elements For Third Party Cyber Risk Management In the Financial Sector," October 2022, https://home.treasury.gov/system/files/216/G7-FUNDAMENTAL-ELEMENTS-FOR-THIRD-PARTY-CYBER-RISK.pdf.

The update includes explicit recommendations for monitoring risks along the supply chain, identifying systemically important third-party providers, and addressing potential concentration risks.

Board Internal

The Board places a strong emphasis on promoting cyber-risk management through active collaboration and coordination across agency stakeholders. To achieve this goal, the Board's Office of the Chief Operating Officer (OCOO) facilitates timely exchange of information regarding cyber-risk issues across divisions, including business, IT, and information security functions. This approach ensures that cross-functional perspectives are taken into account, enabling the Board to coordinate its efforts and develop cohesive cybersecurity policy. Board security personnel take an active role in other coordination activities, collaborating with groups within the System, as well as participating in interagency cybersecurity forums and working groups facilitated by CISA. This collaboration helps Board staff better identify and respond to potential threats. The Board is an active participant in CISA's Continuous Diagnostics and Mitigation (CDM) program, which is a government-wide effort to improve cybersecurity risk management across all federal agencies. The CDM provides tools and services to help agencies identify and prioritize cybersecurity risks, improve visibility into their networks, and make informed decisions about how to address those risks.

Board OIG Assessment of the Board's Progress in Implementing Key FISMA Information Security Program Requirements

To support the annual independent evaluation of agency information security programs by inspectors general (IGs) under FISMA, DHS publishes FISMA reporting metrics. These metrics direct IGs to evaluate the effectiveness of agency information security programs across various attributes grouped into eight security domains.[39] These domains align with the five security functions defined by the NIST Framework for Improving Critical Infrastructure Cybersecurity (Cybersecurity Framework): *identify, protect, detect, respond, and recover*.[40] Pursuant to the FISMA reporting metrics, IGs assess the effectiveness of each of the five NIST Cybersecurity Framework function areas using a maturity model spectrum. The five levels of the IG FISMA maturity model are ad hoc (level 1), defined (level 2), consistently implemented (level 3), managed and measurable (level 4), and optimized (level 5). Within the context of the maturity model, a level 4 information security program is considered as operating at an effective level of security. While more work needs to be done, the Board OIG's 2022 assessment of the Board's overall information security program rated the pro-

[39] See "FY 2020 Inspector General Federal Information Security Modernization Act of 2014 (FISMA) Reporting Metrics, Version 4.0," Cybersecurity and Infrastructure Security Agency, last modified on April 17, 2020, https://www.cisa.gov/sites/default/files/publications/FY_2020_IG_FISMA_Metrics.pdf.

[40] See "Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1," National Institute of Standards and Technology, April 16, 2018, https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf. The NIST Cybersecurity Framework provides agencies with a common structure for identifying and managing cybersecurity risks across the enterprise.

gram as continuing to operate effectively at a level 4 maturity.[41] The Board will continue to prioritize the protection of its operations and assets through ongoing assessments and improvements of its security posture.

The Board's Ongoing Efforts to Strengthen Its Information Security Program

The Board places a strong emphasis on maintaining a comprehensive security and privacy control program, which is supported by a centralized Plan of Action and Milestones (POA&M) process. This process ensures that plans are developed in response to any finding or weakness identified in security and privacy control implementations. In addition, the POA&M process is used to track and report on the remediation of findings and status of recommendations issued by the OIG, as well as weaknesses identified through internal controls testing. Board staff plan to continue to work on making progress on closing outstanding POA&Ms.

The Board is taking steps to improve our cybersecurity posture and protect against cyberthreats. We are investing in technical controls such as firewalls, intrusion detection and prevention systems, and security information and event management systems to monitor and detect potential threats. We are also following FISMA and related NIST standards and guidance and we are implementing the necessary controls to protect our information systems. In addition, we engage with third-party security experts to perform regular assessments and penetration testing to identify opportunities to improve our security posture. Finally, we are implementing a layered security architecture, which includes multiple layers of defense such as network segmentation, access controls, and encryption to better protect non-public information.

The Board is also working on numerous efforts to enhance our information security architecture. Indeed, one of our top priorities includes the implementation of a zero trust security model, which will provide an additional layer of security to protect our systems and data, as well as implementing web application security measures to identify and address vulnerabilities in our web applications. We are also working to enhance our existing policies and procedures to account for necessary security requirements for cloud systems and capabilities, such as updates to our incident response and data protection policies.

[41] See Board of Governors of the Federal Reserve System, Office of Inspector General, *2022 Audit of the Board's Information Security Program* (Washington: Board of Governors, September 2022), https://oig.federalreserve.gov/reports/board-information-security-program-sep2022.pdf.

Current or Emerging Threats to Financial System Resilience

The Board actively monitors cyber risks and emerging threats through the supervisory process, internal Federal Reserve programs and resources, and coordination with financial regulatory agencies and other government agencies and the private sector. Given the highly interconnected nature of the financial services sector and its dependencies on critical service providers, all participants in the financial system face cyberthreats.

The rising number of advanced persistent threats increases the potential for malicious cyber activity within the financial sector. Combined with the increased internet-based interconnectedness between financial institutions and the increasing dependence on third-party service providers, these threats may result in incidents that affect one or more participants in the financial services sector simultaneously and have potentially systemic consequences. Such incidents could affect the ability of targeted firms to provide services and conduct business as usual, presenting a unique challenge to operational resilience. These incidents can also threaten the confidentiality, integrity, and availability of the targeted firm's data.

Given the evolving threat landscape and potential for exploitation of vulnerabilities, domestic financial institutions have maintained a heightened state of preparedness. The Board and other FBAs are closely monitoring developments related to these threats and have not observed any material impacts to the financial sector.

Geopolitical Tensions

The financial sector is potentially vulnerable to foreign conflicts and the activities of nation-state actors both directly and indirectly because of the interconnectedness of global financial markets and reliance on international digital networks. Adverse geopolitical events, such as the Russian invasion of Ukraine, increase the likelihood of cyberattacks with the intent of disrupting critical infrastructure, including financial services, or undermining trust in public and private sector institutions. In particular, distributed denial of service (DDoS)[42] attacks have been widely observed due to the relatively low sophistication the attacks require and their potential to disrupt the availability of information systems if organizations do not have effective information security and resiliency

[42] NIST defines DDoS as a denial-of-service technique that uses numerous hosts to perform cyber-attacks.

controls. Additionally, destructive malware[43] tools and methods used to destroy or corrupt critical data have been employed and observed. These methods are evolving in sophistication and capability.

Cyber Criminal Activity

The global cyber-criminal ecosystem continues to remain a top threat across geographies and industry sectors, including the financial sector within the United States. As ransomware and cyber extortion attacks persist, these attacks may disproportionately affect small community and regional banking organizations that may not have sufficient information security resources and capabilities to protect their banking systems against sophisticated actors. The number of ransomware groups and their activities is dynamic as threat actors emerge and disband for many reasons including the actions undertaken by law enforcement agencies to identify and prosecute threat actors as well as take down their attack platforms. Ransomware groups continue to evolve their techniques and methods as they seek to monetize cyberattacks and exert maximum pressure on victim organizations.

Cyber-criminal methods and resource offerings that pose a risk to financial institutions' ability to operate and protect customer data may include:

- **Ransomware as a service (RaaS)**. Like traditional ransomware, RaaS is an increasing concern with added sophistication, speed of proliferation, and difficulty of attribution. RaaS allows threat actors to create "franchised" threat offerings. Sophisticated threat actors license the use of their software to other malicious actors, often for a percentage of the ransom. This evolving threat model allows less sophisticated threat actors greater opportunity to impact businesses. Organizations that refuse to pay the ransom often need to rebuild infrastructure to restore business operations.
- **Threats targeting weaknesses in authentication mechanisms.** Single-factor authentication is largely insufficient due to credential-based attacks and in some cases the availability of credentials on dark web forums. Some organizations have moved to MFA as a result of these weaknesses. In 2022, threat actors significantly improved their ability to circumvent weaker forms of MFA through several techniques. Organizations that are implementing MFA need to remain aware of threat actor capability and move towards more robust forms of MFA where possible. In 2021, the FFIEC issued "Authentication and Access to Financial Institution Services and Systems," which highlights the benefits and increased effectiveness of MFA for protecting systems and information.[44]

[43] See Cybersecurity and Infrastructure Security Agency, "Update: Destructive Malware Targeting Organizations in Ukraine," news release, April 28, 2022, https://www.cisa.gov/news-events/cybersecurity-advisories/aa22-057a.

[44] See "Authentication and Access to Financial Institution Services and Systems," Federal Financial Institutions Examination Council, August 11, 2021, https://www.ffiec.gov/guidance/Authentication-and-Access-to-Financial-Institution-Services-and-Systems.pdf.

- **Collaboration among cyberthreat actors.** Threat actors have continued to improve their ability to work together to enable more effective and efficient attacks. Cyber criminals will frequently share or sell information as well as tools and services to lower the bar and make it easier for others and, in particular, middle- and lower-tier actors to engage in these attacks.

There are several methods that threat actors utilize to exploit vulnerabilities in software. Malicious actors continue to exploit both "zero-day" vulnerabilities (patches not available) and "n-day" vulnerabilities (patches available but not yet applied). The window between patch availability and exploitation activity continues to shorten because threat actors and security researchers are publishing detailed information about the vulnerabilities within hours or days of the initial discovery. This emphasizes the importance of a defense-in-depth security posture where a breakdown in one control does not lead to widespread compromise.

Increasing Potential of a Supply Chain or Third-Party Attack

A significant evolving risk is the impact of a cyber-attack against a software vendor or third party, coupled with the threat types described above. Supply chain compromise can impact the financial system through the software provided by third parties. This includes proprietary software as well as open-source software.

The ability of threat actors to breach software providers and subsequently use the breached provider's software to compromise the provider's client firms highlights the risks stemming from interdependency often associated with third-party vendor management and automated software updates being applied. This includes software-as-a-service, an ongoing connection between a software provider and a client firm, where the product is remotely updated on a periodic basis. As third-party software, particularly software-as-a-service, becomes increasingly common in banking, cybersecurity risks are multiplied.

The past year has also further increased the importance of reviewing the resiliency of the sector's supply chain and third-party relationships. As highlighted by CISA, new vulnerabilities arose that could facilitate attackers' ability to take over an affected system.[45] It has been reported that attackers can exploit these vulnerabilities to steal data and further compromise organizations.

Cyber Risks Associated with Third-Party Providers

Financial institutions are increasingly relying on third-party service providers for significant business functions. Such providers are also increasingly becoming responsible for functions that are critical to the operations of those financial institutions. While there are benefits to the use of third-

[45] See Cybersecurity and Infrastructure Security Agency, "Cybersecurity Alerts and Advisories," https://www.cisa.gov/news-events/cybersecurity-advisories.

party services, there are also challenges in ensuring adequate oversight of critical services not performed directly within the client financial institution. A vulnerability at one provider could also have a simultaneous impact on multiple client financial institutions.

Financial institutions' increasing dependency on third parties is illustrated by such institutions moving critical services to remote cloud computing platforms to gain benefits such as increased computing capacity, lower costs, and concentrated technical expertise. In 2023, the Treasury published a report outlining trends related to the adoption of cloud services by the financial services sector as well as potential risks and other challenges. Challenges noted in securely implementing a cloud strategy included insufficient transparency to support due diligence and monitoring, gaps in human capital and tools to securely deploy cloud services, exposure to potential operational incidents, potential impact of market concentration, dynamics in contract negotiation given market concentration, and international landscape and regulatory fragmentation. The most common cause of data breaches noted was misconfiguration of the services by the client financial institution which occurs when the client financial institution and the vendor share responsibility for configuring various aspects of the services and the client does not understand its responsibilities.[46]

Financial institutions are also moving critical services to remote cloud computing platforms with risks of exploitation of internet-accessible vulnerabilities in the cloud services that financial institutions rely upon. The Federal Reserve continues to engage with the Treasury and other public and private sector partners to address risks associated with third-party dependencies.

Insider Threats

Financial institutions have been at increased risk of incidents attributed to personnel and contractors since 2020 when the institutions began allowing remote access over the internet into core banking services and operational support systems as well as granting expanded access permissions to allow for remote work. Controls used to protect against unauthorized activities by insiders, such as MFA, have not always been effective in addressing the risk, especially if misconfigured or when vulnerabilities in the systems are discovered. Insider threats present challenges that financial institutions will continue to need to monitor and address.

Other Emerging Technology-Related Threats

Third-party service providers, including fintech firms, can offer consumers the potential for access to new or better services, but such arrangements also provide greater opportunity for malicious actors to gain access to private data. Specifically, such emerging technologies are often vulnerable to exploitation by tech-savvy hackers looking to profit from technical and financial vulnerabili-

[46] See U.S. Department of the Treasury, *The Financial Services Sector's Adoption of Cloud Services* (Washington: Department of the Treasury, 2023), https://home.treasury.gov/system/files/136/Treasury-Cloud-Report.pdf.

ties in these technologies. Of particular potential risk is the rapid adoption by financial institutions of application programming interfaces, which provide accessible gateways into firms' information (often relied on by fintech platforms for information sharing) and may increase the risk of data breaches, especially of customers' personal or sensitive information, if not effectively secured and permissioned.

The adoption and evolution of machine learning tools will also introduce potential new risks. Machine learning capabilities could drive improvements in the automation of information security controls, such as intrusion detection and data loss prevention. Threat actors, however, could also use machine learning capabilities to automate cyber reconnaissance and attacks, further increasing the likelihood and impact of cyber incidents. The recent deployment of machine learning tools, including generative artificial intelligence technologies, may also provide threat actors with improved methods for performing social engineering, email phishing, and text messaging smishing attacks compromising access into firms' systems, emails, databases, and technology services.

Quantum computing is another emerging risk area, as quantum computing capabilities could render current encryption standards used by financial institutions obsolete. The introduction of quantum cryptography will provide new solutions for protecting the integrity and confidentiality of data at rest and in transit but will also give threat actors new capabilities to avoid detection as well as permit data exfiltration. Hardware requirements and other factors may make the widespread implementation of quantum cryptography difficult currently, especially in legacy systems.

Threats such as these highlight the importance of collective actions across government and strong collaboration with the private sector in advancing measures to understand and mitigate risks. Cyber-risk mitigation and cyber resilience initiatives continue to be high priorities for the Federal Reserve. Through policymaking, supervision of financial institutions and other entities overseen or operated by the Federal Reserve, and internal policies aimed at mitigating cyberthreats, the Federal Reserve continues to maintain a strong internal resilience posture and promote resilience among the financial sector as a whole.

Find other Federal Reserve Board publications (www.federalreserve.gov/publications.htm) or order those offered in print (www.federalreserve.gov/files/orderform.pdf) on our website. Also visit the site for more information about the Board and to learn how to stay connected with us on social media.

www.federalreserve.gov
0823